الخليج

اقتصاد, تقنية وسيارات

5 يناير 2024 22:58 مساء

هجمات «الفدية».. عنوان الجرائم السيبرانية 2024

يشعر 96% من مسؤولي حماية المعلومات في الإمارات بثقة أكبر عند التصدي لتهديدات برامج الفدية، التي تُعدّ واحدة من أكبر المشكلات التي تواجههم في الدولة، فيما ذكر 57% أن لديهم برامج فعالة للأمن السيبراني في مؤسساتهم وشركاتهم»، وفقاً لاستبيان أجرته شركة «مانديانت»، التابعة ل«جوجل كلاود».

تتصدر هجمات الفدية السيبرانية المالية قائمة الهجمات الإلكترونية خلال عام 2024، معتمدة على تطور تقنيات الذكاء الاصطناعي القادرة على اختراق طبقات أو جدران حماية المعلومات في المؤسسات والشركات.

أكد خبراء أمن المعلومات أن قراصنة البيانات سيواصلون توظيف الذكاء الاصطناعي للإيقاع بضحاياهم وطلب فدية مالية لإعادة البيانات للمؤسسات والشركات العام المقبل، ما يتطلب مزيداً من تدريب العنصر البشري على استباق القراصنة للحد من الخسائر المالية.

- **أهداف عالية القيمة**

وقال جميل أبو عقل، رئيس هندسة النظم بمنطقة الشرق الأوسط وإفريقيا والمناطق الناشئة: يشير استبيان «مانديانت» إلى أن التصيد الاحتيالي الذي تقوم به عصابات المعلومات بات منظماً بشكل كبير، فضلاً عن وجود جهات ترعاها.

الصورة

وأضاف أبو عقل، أن استهداف شركات أو صناعات محددة بات يسمح لمجرمي الإنترنت بالوصول إلى أهداف عالية القيمة، كما يسمح للقراصنة بجمع معلومات سرية حول موضوعات محددة.

وأوضح أن دولة الإمارات تعد هدفاً مرغوباً فيه لجهات التهديد السيبراني، وذلك بسبب اقتصادها المتقدّم ومركزها البارز في الشرق الأوسط وعلى الساحة العالمية.

وأكد أبو عقل، ضرورة تبني فهم شامل حول جهات التهديد الحالية والناشئة، وتكوين رؤية واضحة وواسعة حول قوة تدابيرها الأمنية وفعاليتها في التصدي لهذه الجهات، إضافة إلى المعارف الضرورية لدعم تلك التدابير، حيث تهدف «مانديانت» إلى زيادة الوعي بأهمية الاستعداد وعدم انتظار وقوع حادث أمني لاختبار مدى جاهزية واستعداد فريق الأمن، كما ننصح الشركات والمؤسسات بالاستفادة من الخبرات والحلول الأحدث لمساعدتها على اكتشاف التهديدات السيبرانية والتحقيق فيها والاستجابة لها بشكل أكثر كفاءة.

• 6 ملايين دولار كلفة الهجمة

وقال زياد نصر، المدير العام الإقليمي لشركة «أكرونيس»: نظراً لموقع الشرق الأوسط على الصعيد العالمي وبالأخص دولة الإمارات وتحولها إلى مركز اقتصادي عالمي، أصبحت شركات القطاعين العام والخاص هدفاً أساسياً للهجمات السيبرانية، حيث تشير بيانات شركة «آي بي إم» بوضوح إلى أن متوسط كلفة الهجمة السيبرانية على المؤسسات في المملكة العربية السعودية ودولة الإمارات يقدّر بنحو 6.53 مليون دولار، بما يزيد على المتوسط العالمي بنسبة 69%.

وأضاف، على مدار السنوات القليلة الماضية، كانت هجمات الفدية هي مصدر القلق الرئيسي، ولكن مع تبني العديد من الإجراءات والتدابير الحازمة وغير المكلفة لتفادي تلك الهجمات، وتوفير حلول تقنية للتعامل معها، تمكّن صناع القرار من التغلب على هذه الهجمات والحد من آثارها الخطيرة.

وأضح نصر أنه من المؤكد أن التعليم المستمر وزيادة القدرات والمهارات البشرية واستثمار الشركات في تدابير الحماية السيبرانية، عبر مختلف القطاعات، من أهم المحاور لتأهيل المنطقة لمجابهة التهديدات السيبرانية المستمرة.

• ضرورة اليقظة التامة

وقال جوني كرم، نائب الرئيس الإقليمي للأسواق الناشئة الدولية في «فيريتاس تكنولوجيز»: تتصدر دولة الإمارات جهود تبني التقنيات الناشئة، مثل الذكاء الاصطناعي لتعزيز المرونة السيبرانية، وعلى الرغم من أن معظم الشركات في الدولة تبدي ثقتها بقدرتها على الحفاظ على أمنها السيبراني، نظراً لتركيزها المتزايد على الاستثمار في اعتماد أحدث

التقنيات وتطوير المهارات البشرية، فإن 57% تعتبر أنها لا تزال «معرّضة للخطر» نتيجة للتهديدات المتزايدة، لذا نرى أن اليقظة التامة والاستثمارات الاستراتيجية أمر بالغ الأهمية في عالم تملؤه التهديدات والمخاطر الخارجية المتصاعدة، لضمان مستقبل آمن ومستقر.

وتابع كرم: سيؤدي تزايد ظهور هجمات برامج الفدية الذاتية التي تعتمد على الذكاء الاصطناعي بالكامل إلى خلق تحديات جديدة للأمن السيبراني، وأظهر استطلاع أجرته الشركة أن 73% من المؤسسات على مستوى الإمارات تعرّضت خلال العامين الماضيين لهجمات فدية، وستستمر هذه الهجمات، من حيث الوتيرة والتطور، بسبب تمكنهم من الاستفادة من التقدم الحاصل في مجال الذكاء الاصطناعي.

وقال كرم إن عام 2024 سيكون عام هجمات برامج الفدية الذاتية التي تعتمد على الذكاء الاصطناعي، بحيث سيعتمد مجرمو الإنترنت على الذكاء الاصطناعي بشكل كامل لتنفيذ هجماتهم السيبرانية، لتشمل: المكالمات الآلية، وتحديد الأهداف بواسطة الذكاء الاصطناعي، وتنفيذ الاختراقات، وابتزاز الضحايا، وجمع الفدية، وسيتم تحقيق كل ذلك بكفاءة ملحوظة وبأقل تدخل للعنصر البشري.

• نمو ميزانيات الحماية % 30

وقال كرم: ستتطور برامج الفدية من حيث الهجمات التي تستهدف إتلاف البيانات، فيما شهدت ميزانيات حماية البيانات في الإمارات زيادة بمقدار الثلث خلال الشهور ال12 الماضية، ونظراً لكون الشركات قد أصبحت أكثر استعداداً للتعافي من هجمات برامج الفدية دون دفع فدية، سيضطر مجرمو الإنترنت إلى مواصلة تطوير أساليبهم الاحتيالية، ومن المتوقع خلال 2024 أن يلجأ المتسللون إلى تطبيق هجمات تستهدف إتلاف البيانات على مستوى الخلية، وهي عبارة شيفرة برمجية سرية تُزرع في عمق قاعدة بيانات الضحية لتستهدف إتلاف بيانات محددة وغير معرّفة للضحية، إذا تم رفض دفع فدية من قبل الضحية، ويكمن خطر وصعوبة هذا النوع من الهجمات في أن الضحايا لن يعرفوا ما هي البيانات التي تم إتلافها، وإن وجدت، فإن تداعيات الهجمة تكون قد ظهر ويصعب تلافيها، والحل الوحيد هنا يكون بالاحتفاظ بنسخ آمنة تم التحقق منها والتأكد بنسبة 100% من عدم تلفها، وأنها قابلة للاستعادة بسرعة.

• أكثر القضايا إلحاحاً وإثارة للقلق

قال أنطوان حرب، مدير فريق الشرق الأوسط في شركة «كينغستون تكنولوجي»: أصبحت قدرات حماية البيانات أكثر أهمية من أي وقت مضى بالنسبة إلى المؤسسات والشركات في مختلف القطاعات. وأوضح حرب، أن الجرائم السيبرانية واحدة من أكثر القضايا إلحاحاً وإثارة للقلق، وتظهر التهديدات الجديدة باستمرار ونلحظ اهتماماً وتصميماً حقيقياً على مواجهة هذه التهديدات، نظراً لآثار الكلفة المترتبة على الفشل في تلبية قواعد ولوائح ومتطلبات حماية البيانات.

وقد قدّم تقرير المؤسسة الدولية للحواسيب «آي بي إم» لكلفة خرق البيانات لعام 2023 توضيحاً صارخاً للعواقب في حالة اختراق المعلومات الصحية المحمية، فسلّط الضوء على متوسط كلفة خرق بيانات الرعاية الصحية على مستوى

العالم، الذي وصل إلى 10.93 مليون دولار 2023، وكان هذا أعلى معدّل بين جميع القطاعات، ويمثل زيادة كبيرة قدرها 53.3% خلال 3 سنوات فقط.

أما في الشرق الأوسط، فإن الكُلف المترتبة على ذلك ليست بعيدة عن الركب، فوصلت إلى 9.186 مليون دولار خلال هذا العام، وهي أعلى من المتوسط القياسي الإقليمي البالغ 8 ملايين دولار الذي يشمل جميع القطاعات.